(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年6 月3 日 (03.06.2004)

PCT

(10) 国際公開番号
WO 2004/046912 A1

(51) 国際特許分類[7]: G06F 7/58

(21) 国際出願番号: PCT/JP2003/014517

(22) 国際出願日: 2003 年11 月14 日 (14.11.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2002-331884
2002 年11 月15 日 (15.11.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO.,LTD.) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2 丁目5 番5 号 Osaka (JP). 株式会社数理設計研究所 (KABUSHIKI KAISHA SURI SEKKEI KENKYUSHO) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 54−2 Gunma (JP).

(72) 発明者; および

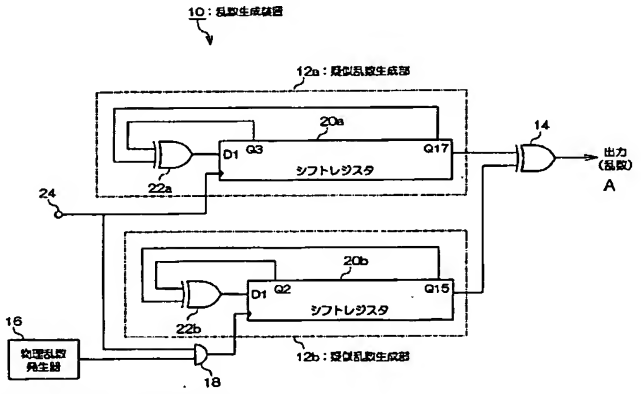
(75) 発明者/出願人 (米国についてのみ): 女屋 正人 (ONAYA,Masato) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2 丁目5 番5 号 三洋電機株式会社内 Osaka (JP). 玉置 晴朗 (TAMAKI,Haruro) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 54−2 株式会社数理設計研究所内 Gunma (JP). 池谷 昭 (IKETANI,Akira) [JP/JP]; 〒110-0005 東京都 台東区上野 1 丁目19 番10 号 三洋セミコンデバイス株式会社内 Tokyo (JP).

(74) 代理人: 吉田 研二, 外 (YOSHIDA,Kenji et al.); 〒180-0004 東京都 武蔵野市吉祥寺本町 1 丁目34 番12 号 Tokyo (JP).

[続葉有]

(54) Title: RANDOM NUMBER GENERATOR

(54) 発明の名称: 乱数生成装置



10...RANDOM NUMBER GENERATOR
12a...PSEUDO RANDOM NUMBER GENERATING UNIT
12b...PSEUDO RANDOM NUMBER GENERATING UNIT
20a...SHIFT REGISTER
20b...SHIFT REGISTER
16...PHYSICAL RANDOM NUMBER GENERATOR
A...OUTPUT (RANDOM NUMBER)

(57) Abstract: A random number generator comprising a plurality of pseudo random number generating units that can respectively output random numbers in specified pseudo random number systems, an output random number generating unit that generates output random numbers based on outputs from a plurality of pseudo random number generating units, a physical random number generator that generates physical random numbers, and a switching unit for switching between the necessity and the non-necessity of updating output values from pseudo random number generating units based on physical random numbers generated by the physical random number generator. Based on which pseudo random number system an output random number is generated is randomly switched based on a physical random number, making it very difficult to predict a random number compared with a conventional one.

(57) 要約: 乱数生成装置は、各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成部と、複数の疑似乱数生成部の出力に基づいて出力乱数を生成する出力乱数生成部と、物理乱数を生成する物理乱数発生器と、物理乱数発生器の生成した物理乱数に基づいて

[続葉有]

WO 2004/046912 A1

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

疑似乱数生成部の出力値の更新の有無を切り替える切替部と、を備える。かかる構成によれば、出力乱数をどの疑似乱数系列に基づいて生成するかが物理乱数に基づいてランダムに切り替わることとなり、従来の乱数に比べ、その予測が非常に難しくなる。

明　細　書

乱数生成装置

技術分野

本発明は、乱数生成装置に関し、特に暗号化アルゴリズムに好適な乱数生成装置に関する。

背景技術

暗号化アルゴリズム等では、セキュリティの確保のために、しばしば乱数が用いられる。その場合の乱数としては、一般的に、M系列（Maximum length code：最長符号系列）等に代表される疑似乱数が用いられてきた。M系列符号は、公知の線形シフトレジスタ符号発生器によって生成することができる。

また、上記疑似乱数以外の乱数として、原子核の崩壊現象がランダムとなることや電気雑音等の自然現象を利用して生成される物理乱数が知られている。暗号化アルゴリズム等においても、上記疑似乱数に替えて、この物理乱数を利用する場合もある（例えば、日本特開２０００－６６５９２号公報参照）。

しかしながら、M系列等に代表される疑似乱数は、必ずしも安全性の高い乱数とは言えず、セキュリティ確保の面からは好ましくない面がある。疑似乱数は、一定の算術プロセスあるいは関数の組み合わせから生成されるため、同じ初期条件を与えれば、同一の乱数を生成可能となるからである。

また、一般的に物理乱数は微弱な信号であるため、暗号化アルゴリズム等で使用するためには、通常、増幅器によって利用可能なレベルに増幅される。ところが、増幅器は電界や磁界によって影響を受ける場合があり、それらの意図的な印加によって乱数の発生確率が操作され、安全性が低下してしまう場合があった。

発明の開示

本発明にかかる乱数生成装置は、各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成手段と、上記複数の疑似乱数生成手段の出力に基づいて出力

乱数を生成可能な出力乱数生成手段と、物理乱数を生成する物理乱数生成手段と、上記物理乱数生成手段の生成した物理乱数に基づいて、上記出力乱数生成手段における出力乱数の生成に、少なくとも一つの上記疑似乱数生成手段で生成される疑似乱数を用いるか否かを切り替える切替手段と、を備える。すなわち、上記本発明にかかる乱数生成装置によれば、複数の疑似乱数系列のうち出力乱数の元となる疑似乱数系列が物理乱数に基づいて変更されるため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測は従来装置に比べてかなり難しくなる。

上記本発明にかかる乱数生成装置では、上記切替手段が、物理乱数に基づいて、少なくとも一つの上記疑似乱数生成手段にクロック信号を入力するか否かを切り替えるように構成してもよい。この構成では、疑似乱数生成手段にクロック信号を入力するか否かを切り替えることで、その疑似乱数生成手段から新たな疑似乱数が出力されるか否かが切り替わる。

また、上記本発明にかかる乱数生成装置では、上記物理乱数生成手段の生成した物理乱数が少なくとも一つの上記疑似乱数生成手段のクロック信号として入力されるように構成してもよい。この構成では、クロック信号としての物理乱数出力の値が切り替わることで、その疑似乱数生成手段から新たな疑似乱数が出力されるか否かが切り替わる。なお、この場合には、上記物理乱数生成手段が上記切替手段として機能することになる。

また、上記本発明にかかる乱数生成装置では、上記切替手段が、物理乱数に基づいて、少なくとも一つの上記疑似乱数生成手段で生成された疑似乱数を上記出力乱数生成手段に入力するか否かを切り替えるように構成してもよい。この構成では、切替手段によって、少なくとも一つの疑似乱数生成手段によって生成された疑似乱数を出力乱数生成手段に入力するか否かを切り替える。

図面の簡単な説明

図１は、本発明の実施の形態１にかかる乱数生成装置の構成図である。

図２は、本発明の実施の形態にかかる乱数生成装置で用いられる物理乱数発生器の構成図である。

図３は、本発明の実施の形態２にかかる乱数生成装置の構成図である。

図４は、本発明の実施の形態３にかかる乱数生成装置の構成図である。

図５は、本発明の実施の形態４にかかる乱数生成装置の構成図である。

発明を実施するための最良の形態

実施の形態１．　図１は、本実施形態にかかる乱数生成装置１０の構成を示す図、また図２は、物理乱数発生器１６の構成図である。

乱数生成装置１０は、二つの疑似乱数生成部１２ａ，１２ｂ、出力乱数生成部１４、物理乱数発生器１６、および切替部１８を含む。このうち疑似乱数生成部１２ａ，１２ｂは、それぞれ、縦続して接続された複数のフリップフロップを含むシフトレジスタ２０ａ，２０ｂと、所定の複数のタップ位置からの出力値の排他的論理和を出力するＥＸＯＲゲート２２ａ，２２ｂと、を有し、所定のM系列の乱数を出力する線形シフトレジスタ符号発生器として構成されている。図１の例では、シフトレジスタ２０ａは、１７個のフリップフロップを有しクロック信号に応じてビットシフトする１７段シフトレジスタであり、入力側より第３番目と第１７番目のフリップフロップからのタップ出力（Ｑ出力；Ｑ３，Ｑ１７）に基づいて帰還入力値（シフトレジスタ２０ａのＤ１入力；「１」（ハイレベル）または「０」（ローレベル））が生成される。また、シフトレジスタ２０ｂは、１５個のフリップフロップを有しクロック信号に応じてビットシフトする１５段シフトレジスタであり、入力側より第２番目と第１５番目のフリップフロップからのタップ出力（Ｑ２，Ｑ１５）に基づいて帰還入力値が生成される。シフトレジスタ２０ａ，２０ｂの段数および帰還入力の元となるタップ位置は互いに異なっており、疑似乱数生成部１２ａ，１２ｂは、相異なるM系列符号を生成することができる。

本実施形態では、疑似乱数生成部１２ａが動作するためのクロック信号（シフトレジスタ２０ａがビットシフトを行うためのクロック信号）は、信号源２４より直接入力されるが、疑似乱数生成部１２ｂ（シフトレジスタ２０ｂ）のクロッ

ク信号は、信号源２４より切替部１８を介して入力される。切替部１８は、物理乱数発生器１６からの物理乱数出力に基づいて、疑似乱数生成部１２ｂにクロック信号を入力するか否かを切り替える。図１の例では、切替部１８はＡＮＤゲートとして構成され、信号源２４からの共通クロック信号の値が「１」であり、かつ物理乱数出力値が「１」であるときにのみ、疑似乱数生成部１２ｂに入力するクロック信号の値（すなわち出力値）を「１」とする。疑似乱数生成部１２ｂは、入力されるクロック信号の値が「１」（ハイレベル）であるときにのみ新たな疑似乱数を出力する（疑似乱数を更新する）から、疑似乱数生成部１２ｂで生成された疑似乱数は物理乱数出力値が「１」であるときにのみ出力乱数生成部１４に入力され、他方、物理乱数出力値が「０」であるときは、その出力値は出力線につながるビットの値（図１の例では第１５番目のビットのＱ１５出力；「１」または「０」）で固定されることとなる。

そして、出力乱数生成部１４において、二つの疑似乱数生成部１２ａ，１２ｂの出力値に基づいて出力乱数が生成される。図１の例では、出力乱数生成部１４は、ＥＸＯＲゲートとして構成され、疑似乱数生成部１２ａ，１２ｂからの出力値が不一致であるときには出力値を「１」とし、他方、それらが一致するときには出力値を「０」とする。ここで、上述したように、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ｂの出力値は疑似乱数となり、他方、物理乱数出力値が「０」であるときは、疑似乱数生成部１２ｂの出力値は「１」または「０」で固定される。つまり、出力乱数生成部１４の出力乱数は、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ａ，１２ｂの双方で生成された疑似乱数に基づいて生成されることとなり、物理乱数出力値が「０」であるときは、疑似乱数生成部１２ａによって生成された疑似乱数に基づいて生成されることとなる。すなわち、本実施形態によれば、出力乱数をどの疑似乱数を用いて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。さらに、本実施形態では、複数の疑似乱数生成部１２ａ，１２ｂによって相異なる疑似乱数が生成されるので、それら複数の疑似乱数生成部１２ａ，１２ｂの双方に基づいて生成された出力乱数自体の予測も難しく、結果として出力乱数の予測は極めて難しく

なる。

ところで、物理乱数発生器１６は、物理乱数発生源１６ａ、増幅回路１６ｂおよび二値化回路１６ｃを備える。このうち、物理乱数発生源１６ａは、自然現象に基づいてランダムに変化する信号を生じうるものであり、例えば、上記特許文献１に開示されるような、接合を含む電流路に生じる雑音信号を生じる半導体素子を含むものとすることができる。なお、これには限られず、放射性物質の崩壊を利用したもの等もこの物理乱数発生源１６ａとして用いることができる。物理乱数発生源１６ａにて生じた信号は、増幅回路１６ｂにおいて増幅され、さらに二値化回路１６ｃにおいて二値化処理される。二値化回路１６ｃは、所定のサンプリングタイミングで、増幅された信号の振幅と所定の閾値とを比較し、例えば、増幅された信号の振幅が所定の閾値より高いときには「１」を、逆に低いときには「０」を出力する。こうして物理乱数発生器１６により、「１」または「０」を示す所定電圧の物理乱数出力値が生成される。なお、二値化回路１６ｃの閾値のレベルは任意に設定することができるが、通常は「１」および「０」の発生確率がほぼ１対１となるように設定される。なお、二値化回路１６ｃにおいて、単に、増幅された信号の振幅を所定の閾値と比較して出力信号を発生するようにしてもよい。

実施の形態２．　図３は、本実施形態にかかる乱数生成装置３０の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

上記実施の形態１では、疑似乱数生成部１２ｂには、クロック信号として、物理乱数発生器１６からの物理乱数出力と信号源２４からの共通クロック信号との論理積を入力したが、本実施形態では、疑似乱数生成部１２ｂへのクロック信号を、物理乱数発生器１６からの物理乱数出力そのものとしている。本実施形態では、物理乱数発生器１６が切替部に相当する。なお、疑似乱数生成部１２ａのクロック信号ＣＫは物理乱数出力とは独立して入力される。このような構成とした場合も、上記実施の形態１と同様の効果が得られる。すなわち、物理乱数出力値が「１」であるときには、疑似乱数生成部１２ｂは、物理乱数出力の出力タイミング（＝物理乱数発生器１６のサンプリングタイミング）で、順次、疑似乱数を

生成し、これが出力乱数生成部１４に向けて出力される。他方、物理乱数出力値が「０」であるときには疑似乱数生成部１２ｂは動作せず、その出力値は出力線につながるビットの値（図３の例では第１５番目のビットのＱ１５出力；「１」または「０」）で固定される。すなわち、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ｂからクロック信号に応じて疑似乱数が出力され、物理乱数出力値が「０」であるときは、疑似乱数が出力されず出力値が固定された状態となる。それら各状態において出力乱数生成部１４から出力される出力乱数は上記実施の形態１と同じとなる。本実施形態でも、上記実施の形態１と同様に、出力乱数をどの疑似乱数を用いて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。なお、物理乱数発生器１６は、サンプリングタイミングで出力するのではなく、任意のタイミングで出力するように構成してもよい。

実施の形態３．　図４は、本実施形態にかかる乱数生成装置４０の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態では、疑似乱数生成部１２ｂで生成した疑似乱数が出力乱数生成部１４に入力されるか否かが切替部４８によって制御される。図４の例では、疑似乱数生成部１２ｂの出力は、ＡＮＤゲートとして構成される切替部４８を介して出力乱数生成部１４に入力されるようになっている。そして切替部４８において、物理乱数発生器１６からの物理乱数出力と疑似乱数生成部１２ｂの出力との論理積が取得され、これが出力乱数生成部１４に入力される。すなわち、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ｂで生成された疑似乱数がそのまま出力乱数生成部１４に入力され、出力乱数生成部１４は、疑似乱数生成部１２ａ，１２ｂ双方の疑似乱数の排他的論理和を取得し、これを出力乱数として出力する。他方、物理乱数出力値が「０」であるときは、出力乱数生成部１４には「０」が入力され、出力乱数生成部１４からは、疑似乱数生成部１２ａの出力値と同じ値の出力乱数（すなわち疑似乱数生成部１２ａの出力した疑似乱数）が出力される。本実施形態でも、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ｂからクロック信号（例えば疑似乱数生成部１２ａと共通のクロック

信号）に応じて疑似乱数が出力され、物理乱数出力値が「０」であるときは、疑似乱数が出力されず出力値が固定された状態となる。つまり、本実施形態でも、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。

実施の形態４．　図５は、本実施形態にかかる乱数生成装置５０の構成を示す図である。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態では、疑似乱数生成部１２ａ，１２ｂでそれぞれ生成された疑似乱数が出力乱数生成部１４に入力されるか否かが物理乱数出力値によって切り替わる。なお、図５の例の場合、疑似乱数生成部１２ａ，１２ｂの生成した疑似乱数のうちいずれか一方が選択的に出力乱数生成部１４に入力され、選択入力された疑似乱数がそのまま出力乱数生成部１４の出力、すなわち乱数生成装置５０の出力となっている。つまり、図５の例では、複数の疑似乱数生成部１２ａ，１２ｂによってそれぞれ生成される疑似乱数パターンのうちどれを出力するかを、物理乱数によって選択的に切り替えていると言うこともできる。具体的には、切替部５８は、二つのＡＮＤゲート５８ａ，５８ｂを備えており、そのうち一方のＡＮＤゲート５８ａには、疑似乱数生成部１２ａの出力と物理乱数発生器１６からインバータ５８ｃを介して物理乱数出力値が入力され、もう一方のＡＮＤゲート５８ｂには、疑似乱数生成部１２ｂの出力と物理乱数発生器１６からの物理乱数出力値が入力される。そして、これら二つのＡＮＤゲート５８ａ，５８ｂの出力が出力乱数生成部１４に入力され、それらの排他的論理和が出力乱数となる。そして、この構成では、物理乱数出力値が「１」であるときは、疑似乱数生成部１２ｂで生成された疑似乱数がそのままＡＮＤゲート５８ｂの出力として出力乱数生成部１４に入力され、他方ＡＮＤゲート５８ａの出力は「０」となる。すなわちこの場合、出力乱数生成部１４からは、疑似乱数生成部１２ｂの出力値と同じ値の出力乱数（すなわち疑似乱数生成部１２ｂの出力した疑似乱数）が出力される。他方、物理乱数出力値が「０」であるときは、疑似乱数生成部１２ａで生成された疑似乱数がそのままＡＮＤゲート５８ａの出力として出力乱数生成部１４に

入力され、他方ＡＮＤゲート５８ｂの出力は「０」となる。すなわちこの場合、出力乱数生成部１４からは、疑似乱数生成部１２ａの出力値と同じ値の出力乱数（すなわち疑似乱数生成部１２ｂの出力した疑似乱数）が出力される。本実施形態でも、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数によってランダムに変化することとなり、従来の物理乱数あるいは疑似乱数に比べて、その予測が非常に難しくなると言える。

以上、本発明の好適な実施形態について説明したが、本発明は上記実施形態には限定されず、種々の等価回路によっても実施可能である。例えば、上記実施形態では、疑似乱数が、１７段または１５段のシフトレジスタを有する線形シフトレジスタ符号発生器によって生成される数種類のM系列符号である場合を例示したが、この例には限定されず、それ以外の段数のシフトレジスタあるいはタップの組み合わせに基づく疑似乱数系列であってもよい。また、複数の疑似乱数生成部を、同じ系列の疑似乱数を発生させるものとしてもよい。また、上記実施形態では、シフトレジスタの最終段のフリップフロップのＱ出力を疑似乱数として出力したが、他のフリップフロップから疑似乱数を出力してもよいし、シフトレジスタに入力される帰還値を疑似乱数出力としてもよい。

産業上の利用可能性

以上説明したように、本発明によれば、出力乱数をどの疑似乱数に基づいて生成するかが物理乱数に基づいてランダムに変化するため、より予測の難しい乱数を生成することができる。このため、例えば、より高い安全性が要求される暗号化技術等での使用に適している。

請 求 の 範 囲

１．各々所定の疑似乱数系列の乱数を出力可能な複数の疑似乱数生成手段と、

前記複数の疑似乱数生成手段の出力に基づいて出力乱数を生成可能な出力乱数生成手段と、

物理乱数を生成する物理乱数生成手段と、

前記物理乱数生成手段の生成した物理乱数に基づいて、前記出力乱数生成手段における出力乱数の生成に、少なくとも一つの前記疑似乱数生成手段で生成される疑似乱数を用いるか否かを切り替える切替手段と、

を備える乱数生成装置。

２．前記切替手段は、物理乱数に基づいて、少なくとも一つの前記疑似乱数生成手段にクロック信号を入力するか否かを切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

３．前記物理乱数生成手段の生成した物理乱数が少なくとも一つの前記疑似乱数生成手段のクロック信号として入力されることを特徴とする請求の範囲第１項に記載の乱数生成装置。

４．前記切替手段は、物理乱数に基づいて、少なくとも一つの前記疑似乱数生成手段で生成された疑似乱数を前記出力乱数生成手段に入力するか否かを切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

５．前記出力乱数生成手段は、排他的論理和ゲートであることを特徴とする請求の範囲第１項に記載の乱数生成装置。

図1

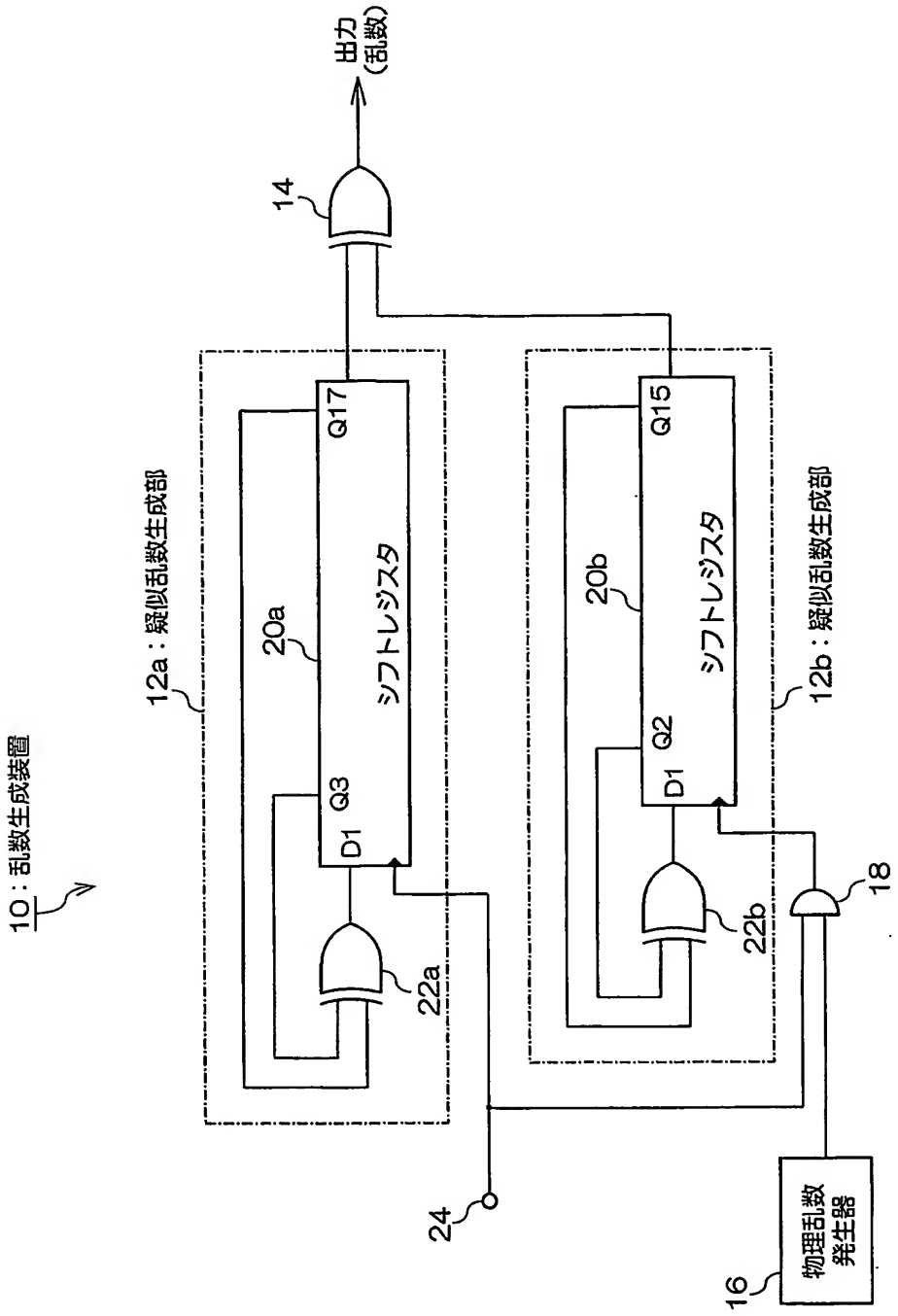

出力
(乱数)
14
12a：疑似乱数生成部
12b：疑似乱数生成部
10：乱数生成装置
20a
シフトレジスタ
Q17
Q3
D1
22a
20b
シフトレジスタ
Q15
Q2
D1
22b
18
24
16
物理乱数
発生器

図2

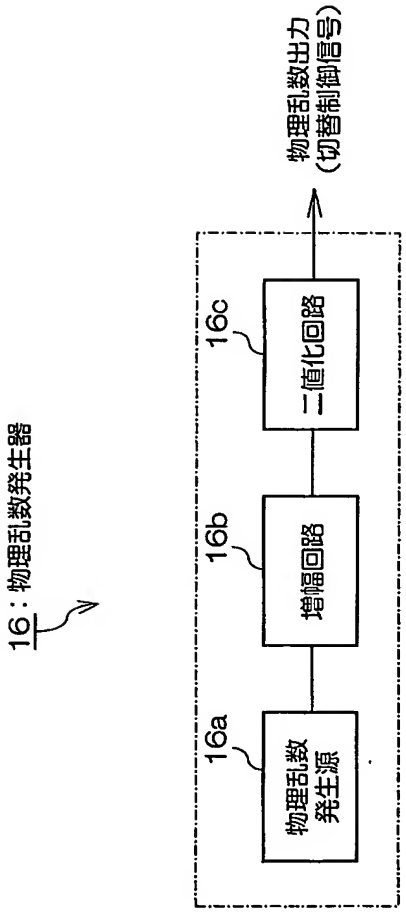


図3

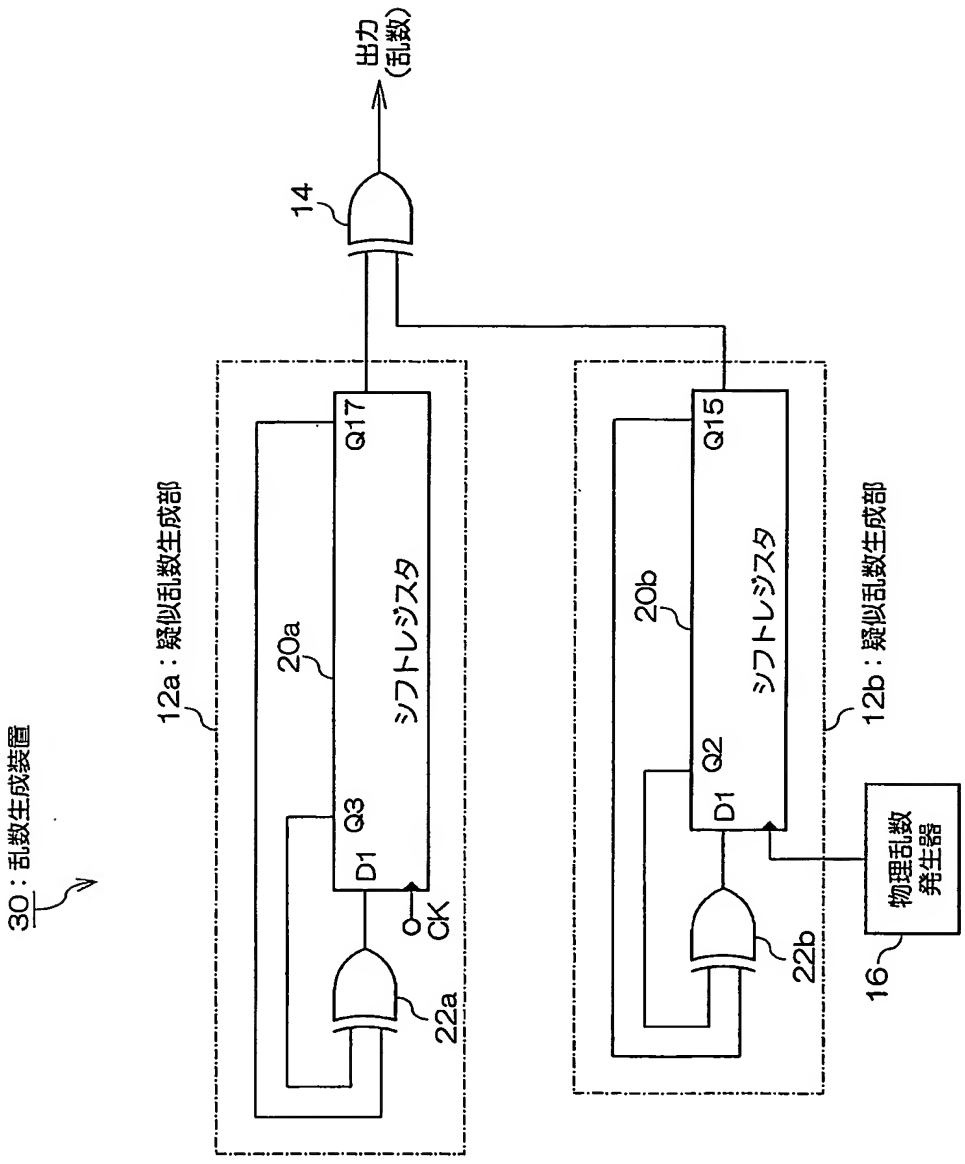

30：乱数生成装置
12a：疑似乱数生成部
12b：疑似乱数生成部
20a
20b
シフトレジスタ
シフトレジスタ
Q17
Q15
Q3
Q2
D1
D1
CK
14
出力
(乱数)
22a
22b
16
物理乱数
発生器

図4

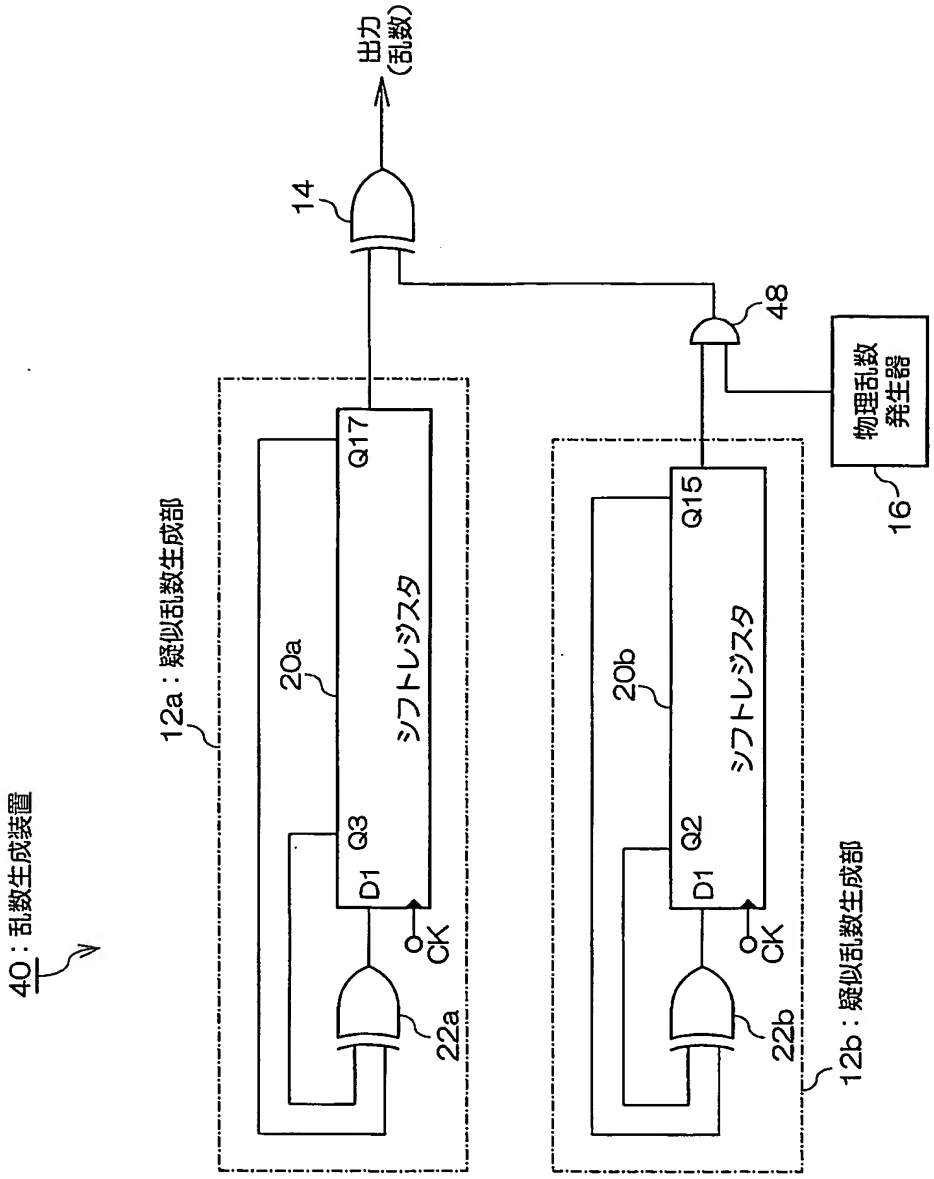
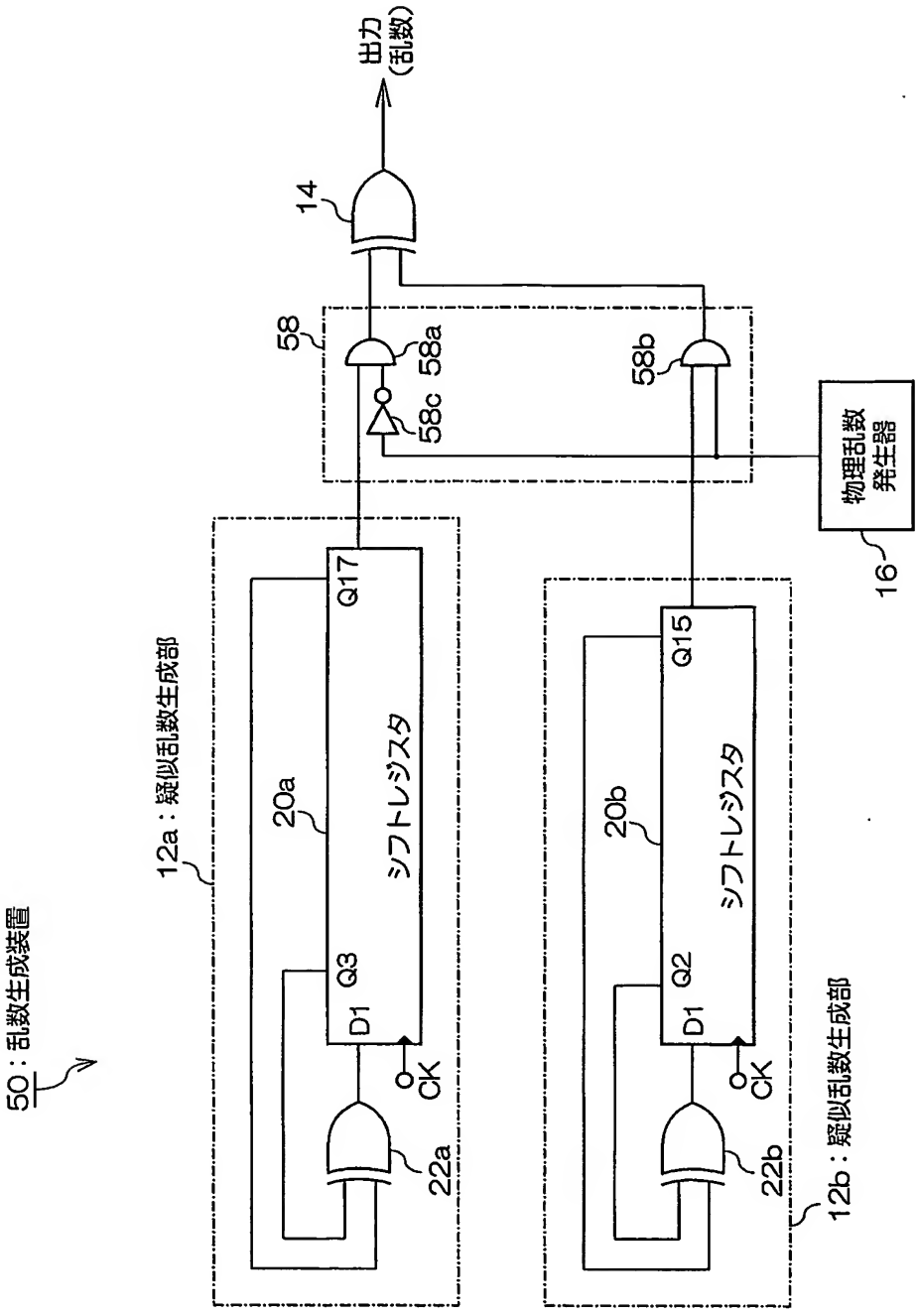

出力
(乱数)
14
48
物理乱数
発生器
16
12a：疑似乱数生成部
20a
シフトレジスタ
Q17
Q3
D1
CK
22a
12b：疑似乱数生成部
20b
シフトレジスタ
Q15
Q2
D1
CK
22b
40：乱数生成装置

図5


50：乱数生成装置
12a：疑似乱数生成部
12b：疑似乱数生成部
20a
20b
シフトレジスタ
Q17
Q15
Q3
Q2
D1
CK
22a
22b
58
58a
58b
58c
14
出力
(乱数)
物理乱数
発生器
16